数理解析研究所講究録
第2008巻 2016年 47-51

Undecidability of the complexity of rewriting systems *

YUJI KOBAYASHI

Department of Information Science,
Toho University
Funabashi 274–8510, Japan

1 Introduction

A rewriting system is a simple but powerful abstract model of computation. When we consider models of computation, fundamental problems are termination and complexity. In our paper in [2], We studied the complexity of string rewriting systems and give conditions for a function to become the complexity of a finite rewriting system. In this note we show that it is principally impossible to determine the complexity of a given finite rewriting system. More precisely, even if we know that a given system has either quadratic or cubic complexity, we cannot decide which one it has.

2 Preliminaries

Let Σ is a (finite) alphabet and let Σ^* be the free monoid generated by Σ. An element $x \in \Sigma^*$ is called a word over Σ and $|x|$ denotes its length. For $n \geq 0$, Σ^n denotes the set of words of length n over Σ.

A (*string*) *rewriting system* on Σ is a subset R of $\Sigma^* \times \Sigma^*$. An element $r = (u, v)$ of R is called a *rule* and written $u \to v$. If a word $x \in \Sigma^*$ contains the left-hand side u of the rule r as a subword, that is, $x = x_1 u x_2$ for some $x_1, x_2 \in \Sigma^*$, then we can apply the rule r to x and x is rewritten to the word $y = x_1 v x_2$. In this situation we write $x \to_r y$. If there is $r \in R$ such that $x \to_r y$, we write $x \to_R y$, and we call $\to_R$ the *reduction relation induced by* R. If any rule in R cannot be applied to x, x is called *R-irreducible*.

A rewriting system R is *terminating on* $x \in \Sigma^*$, if there is no infinite reduction sequence $x \to_R x_1 \to_R \cdots \to_R x_n \to_R \cdots$ starting with x. If R is terminating on any $x \in \Sigma^*$, R itself is called *terminating*. For $x, y \in \Sigma^*$ if there

*This is a preliminary version, and a final version will appear elsewhere.

is a reduction sequence of length n from x to y, we write $x \to_R^n y$. In particular, $\to^0$ is the equality relation and $\to_R^1 = \to_R$. Set $\to_R^* = \cup_{n\geq 0} \to_R^n$.

The maximal length of reduction sequences starting from $x \in \Sigma^*$ is denoted by $\delta_R(x)$;

$$\delta_R(x) = \max\{n \in \mathbb{N} \mid x \to^n y \text{ for some } y \in \Sigma^*\}.$$

If R is not terminating on x, then $\delta_R(x) = \infty$. The (*derivational*) *complexity* of R is the function $d_R : \mathbb{N} \to \mathbb{R} \cup \{\infty\}$ defined by

$$d_R(n) = \max\{\delta_R(x) \mid x \in \Sigma^n\}$$

(see Hofbauer and Lautermann [1] and Kobayashi [2]).

For two functions $f, g : \mathbb{N} \to \mathbb{R} \cup \{\infty\}$, if there is a constant $C > 0$ such that $f(n) \leq Cg(n)$ (resp. $f(n) \geq Cg(n)$) for any sufficiently large $n \in \mathbb{N}$, we write $f = O(g)$ (resp. $f = \Omega(g)$). If both $f = O(f)$ and $f = \Omega(g)$ hold, f and g are *equivalent* and we write as $f = \Theta(g)$.

Example 1. *Let $\Sigma = \{a, b\}$ in (1) and (3) and $\Sigma = \{a, b, c\}$ in (2) below.*

(1) Let $R_1 = \{ab \to ba\}$, then $d_{R_1}(n) = \Theta(n^2)$ because we have a sequence

$$a^n b^n \to^n ba^n b^{n-1} \to^n b^2 a^n b^{n-2} \to^n \cdots \to^n b^n a^n$$

of length n^2.

(2) Let $R_2 = \{ab \to ba, ac \to cb, bc \to ca\}$, then $d_{R_2}(n) = \Theta(n^3)$ because we have a sequence

$$a^n b^n c^n \to^{n^2} b^n a^n c^n \to^n b^n ca^n c^{n-1} \to^n ca^n b^n c^{n-1} \to^{n^2} \cdots \to^n c^n a^n b^n \to^{n^2} c^n b^n a^n$$

of length $n^3 + 3n^n$.

(3) Let $R_3 = \{ab \to b^2 a\}$, then $d_{R_3}(n) = \Theta(2^n)$ because we have a sequence

$$a^n b \to a^{n-1} b^2 a \to^2 a^{n-2} b^4 a^2 \to^4 \cdots \to^{2^{n-1}} b^{2^n} a^n$$

of length $2^n - 1$.

3 Undecidability

Let L be a recursively enumerable non-recursive subset of Σ^*. Let $M(\Sigma, q_i, q_f, Q, \delta)$ be a deterministic single-tape Turing machine that halts with input $w \in \mathrm{L}$ but does not halts with input $w \in \Sigma^* \setminus L$. Here, Q is a finite set of states, q_i is the initial state, q_f is the final state and $\delta : (Q \setminus \{q_f\}, \Sigma_b) \to (Q, \Sigma_b \cup \{\lambda, \rho\})$ is the transaction function of M, where b is the blank symbol, $\Sigma_b = \Sigma \cup \{b\}$ and λ (resp. ρ) is the symbol for the left (resp. right) move of the head. We may assume that the head does not move to the left of its initial position and the head is in the initial position when the machine halts.

For $w \in \Sigma^*$ we define a rewriting system R_w over the alphabet

$$\Omega = \Sigma_b \cup Q \cup \{A, B, E.S, T, R, F\}$$

as follows. Letting $a, a', c \in \Sigma_b$, $q, q' \in Q$, R_w consists of the rules

$$
\begin{array}{lcll}
qAa & \to & q'a'B & \text{if } \delta(q,a) = (q',a'), \\
qAa & \to & aq'B & \text{if } \delta(q,a) = (q',\rho), \\
cqAa & \to & q'caB & \text{if } \delta(q,a) = (q',\lambda), \\
aA & \to & Aa, & \\
Ba & \to & aB, & \\
BE & \to & Ab, & \\
q_fA & \to & q_fS & \\
Sa & \to & aS & \\
SE & \to & Ab, & \\
SF & \to & R, & \\
aR & \to & RE, & \\
q_fR & \to & q_iAw. &
\end{array}
$$

Let $m > 0$, $x \in \Sigma^m$ and $x = x'a$ with $a \in \Sigma_b$, and let $q \in Q \setminus \{q_f\}$. If $\delta(q,a) = (q',a')$ with $q' \in Q, a' \in \Sigma_b$, then we have

$$qAxE \to q'a'Bx'E \to^{m-1} q'a'x'BE \to q'a'x'Ab \to^m q'Aa'x'b \tag{1}$$

in $2m+1$ steps. If $\delta(q,a) = (q',\rho)$,

$$qAax'E \to aq'Bx'E \to^{2m-1} aq'Ax'b \tag{2}$$

in $2m$ steps. Let $c \in \Sigma$. If $\delta(q,a) = (q',\lambda)$,

$$cqAax'E \to q'caBx'E \to^{2m+1} q'Acax'b \tag{3}$$

in $2m+2$ steps.

Suppose that M is in a state q after it acts for t steps. Let $k \in \mathbb{N}$. If $k \geq t$, then by (1) – (3) we see

$$q_iAxE^k \to^* yqAzE^{k-t} \tag{4}$$

for some $y, z \in \Sigma_b^*$ with $|y| + |z| = m + t$ in between $2mt$ and $2(m+2t)t$ steps. If $k < t$, then

$$q_iAxE^k \to^* yqAz \tag{5}$$

for some $y, z \in \Sigma_b^*$ with $|y| + |z| = m + k$ in between $2mk$ and $2(m+2k)k$ steps, and the last term $yqAz$ in (5) is rewritten to the irreducible $y'q'z'B$ in $|z|$ steps for some $y', z' \in \Sigma_b^*$ and $q' \in Q$. Hence, if $x \notin L$, that is, M does not halt with input x, then

$$\delta(q_iAxE^k) = \Theta((m+k)k). \tag{6}$$

On the other hand we have

$$
\begin{aligned}
q_fAxE^k &\to q_fSxE^k \to^m q_fxSE^k \to q_fxAbE^{k-1} \\
&\to^m q_fAxbE^{k-1} \to^{2(m+2)} q_fAxb^2E^{k-2} \to^{2(k+3)} \\
&\cdots \to^{2(m+k)} q_fAxb^k \to q_fSxb^k \to^{m+k} q_fxb^kS
\end{aligned} \tag{7}
$$

in $\Theta((m+k)k)$ steps. Hence, if $\ell > 0$, then

$$q_f AxE^k F^\ell \to^* q_f xb^k SF^\ell \to q_f xb^k RF^{\ell-1} \to^{m+k} q_f RE^{m+k} F^{\ell-1} \to q_i AwE^{m+k} F^{\ell-1} \tag{8}$$

in $\Theta((m+k)k)$ steps.

Suppose that $x \in L$, and M halts in t steps with input x. Let $k \geq t$, then by (5) and (8) we have

$$q_i AxE^k F^\ell \to^* q_f AyE^{k-t} F^\ell \to^* q_i AwE^{m+k} F^{\ell-1} \tag{9}$$

for some $y \in \Sigma_b^*$ with $|y| = m+t$ in $\Theta((m+k)k)$ steps. Here, if $w \notin L$, then by (6) and (9) we have

$$\delta(q_i AxE^k F^\ell) = \Theta((m+k)k). \tag{10}$$

Combining (6) and (10) we see

$$d_{R_w}(n) = \Omega(n^2).$$

Because there is no sequence of length exceeding quadratic order when $w \notin L$, we have

$$d_{R_w}(n) = \Theta(n^2). \tag{11}$$

Now suppose that $w \in L$, and M halts in t steps with input w, then by (9) we have

$$q_i AwE^n F^n \to^{\Theta(n^2)} q_i AwE^{n+m_0} F^{n-1} \to^{\Theta(n^2)} \cdots \to^{\Theta(n^2)} q_i AwE^{n(m_0+1)} \tag{12}$$

in $\Theta(n^3)$ steps, where $m_0 = |w|$. By (4) the last term in (12) is rewritten to $q_f AvE^{n(m_0+1)-t}$ for some $v \in \Sigma_b^*$ with $|v| = m_0 + t$ in $O(1)$ steps, and this last term is still rewritten to irreducible $q_f vb^{n(m_0+1)-t} S$ in $O(n^2)$ steps . Therefore,

$$\delta_{R_w}(q_i AwE^n F^n) = \Omega(n^3).$$

Because there is no sequence of length exceeding cubic order, we see

$$d_{R_w}(n) = \Theta(n^3). \tag{13}$$

By (11) and (13) we get

Lemma 1. *If $w \in L$, R_w has cubic complexity, and if $w \notin L$, R_w has quadratic complexity.*

Because L is non-recursive, Lemma 1 implies

Theorem 2. *For the class **C** of finite rewriting systems with derivational complexity either quadratic or cubic, it is undecidable a given system in **C** has quadratic complexity.*

References

[1] D. Hofbauer, C. Lautermann, Termination proofs and the length of derivations, in: RTA1989, in: LNCS **355**, (1989), 167–177.

[2] Y. Kobayashi, The derivational complexity of string rewriting systems, Theoret. Comp. Sci. **438** (2012), 1 – 12.